MORRISON

Algebraic Numbers

Mathematics

M. A.

1 9 0 8

ALGEBRAIC NUMBERS

BY

HARRY C. MORRISON, A.B. (IND. UNIV.) 1907

THESIS

SUBMITTED IN PARTIAL FULFILLMENT OF THE
REQUIREMENTS FOR THE DEGREE OF

MASTER OF ARTS

IN MATHEMATICS

IN THE

GRADUATE SCHOOL

OF THE

UNIVERSITY OF ILLINOIS

1908

UNIVERSITY OF ILLINOIS

190

THIS IS TO CERTIFY THAT THE THESIS PREPARED UNDER MY SUPERVISION BY

Harry C. Morrison

ENTITLED ALGEBRAIC NUMBERS

IS APPROVED BY ME AS FULFILLING THIS PART OF THE REQUIREMENTS FOR THE

DEGREE OF MASTER OF ARTS IN MATHEMATICS

G. A. Miller

Instructor in Charge.

APPROVED: *E. J. Townsend*

HEAD OF DEPARTMENT OF MATHEMATICS.

CONTENTS.

CHAPTER I .

CHAPTER I I.

THEOREMS RELATING TO GENERAL PROPERTIES OF ALGEBRAIC NUMBERS.

CHAPTER III

QUADRATIC NUMBERS.

CHAPTER IV.

IDEALS IN THE QUADRATIC DOMAIN.

CHAPTER I.

1. Historical Notes.

The early investigations relating to number theory were generally restricted to the natural numbers, that is, to the numbers which result from counting or enumerating. We have evidence that the ancient Romans represented natural numbers by strokes or objects. Livy speaks of driving a nail each year into a certain spot in the sancutary of Minerva, to show the number of years which had elapsed since the building of the edifice. We have evidence also that the people who occupied Mexico before its conquest by the Spainards, possessed natural number signs for all numbers from 1 to 19, which they formed by combinations of circles.

The fraction is present in the oldest deciphered work on Mathematics, viz., the Ahmez papyrus which was written about 1700 B.C. and is itself based upon a much older work. The fractional notation of the Babylonian Astronomers is of great interest historically. Like their notation of integers, it is a sexagesimal positional notation. The denominator is always 60 or some power of 60 indicated by the position of the numerator which alone is written. The fraction $1/8$, for instance, which is equal to $7/60 + 30/60^2$, would in this notation be written 7,30.

2. Definitions.

Real numbers are divided into two classes:rational numbers and irrational numbers. A rational number is a number which may be written in the form p/q where p and q are relatively prime. When q ≠ 1 such a number is called a rational fraction. It is always possible to construct an equation of the first degree whose root is an arbitrary rational number. By irrational numbers we mean all those numbers which are not rational. For the solution of Algebraic equations of a higher degree than the first, irrational numbers are often neccessary. For example even in the simple equation $x^2 = 2$, we have need of an irrational number, namely $\sqrt{2}$. Irrational quantities were known to the Greeks and are generally attributed to the Pythagorean School. The Greeks, however, did not consider irrational numbers. The East Indians were the first to reckon with irrational square roots as with numbers. Bhåskara extracted square roots of binomial surds and rationalized irrational denominators of fractions even when these were polynomial. Only recently has the theory of irrational numbers been developed satisfactori ly. Cantor wrote extensively on this subject beginning in 1871.

Numbers may also be classified as Algebraic and Transcendental. If we have an algebraic equation of the nth degree

$$a_0 x^n + a_1 x^{n-1} + \cdots \cdots \cdots + a = 0$$

in which the coefficients are all rational finite numbers, then a root of such an equation is called an Algebraic Number. If

the coefficient of the highest power is unity and the remaining coefficients are rational finite integral numbers then a root of the above equation is called an Algebraic Integer. All numbers which are not algebraic are called Transcendental. e,g., π, e. There are more transcendental numbers than algebraic numbers, but comparatively little is known about them. π and e are the two transcendental numbers with which we are most familiar.

A Quadratic Number is an algebraic number which satisfies an equation of the second degree. A quadratic integer is an algebraic integer which satisfies an equation of the second degree.

A Domain Of Rationality, or A Number Field is a totality of elements which is invariant with respect to the operations of addition, subtraction, multiplication and division (division by zero being excluded). The Domain Unity, R(1),is composed of the rational numbers. If we take any arbitrary integral number ,m, which contains no quadratic factor, and form a Domain$\sqrt{m}$,such a domain is called a Quadratic Domain.

CHAPTER II.

Theorems Relating to General Properties of Algebraic Numbers.

Theorem I. - If α and β are any two Algebraic Numbers, then $\alpha + \beta$, $\alpha - \beta$, $\alpha\beta$, $\frac{\alpha}{\beta}$, (where in the last case $\beta \neq 0$) are Algebraic Numbers also.

If we have α and β, roots of two equations,

(1)
$$X^m + A_1 X^{m-1} + A_2 X^{m-2} ------------ + A_m = 0$$
$$X^n + B_1 X^{n-1} + B_2 X^{n-2} ------------ + B_n = 0.$$

respectively, where the coefficients are rational numbers, then we may place mn = p, and denote the p products $\alpha^\mu \beta^\nu$ which correspond to the exponents $\mu = 0, 1, 2, 3, ------- m - 1$, $\nu = 0$, 1, 2, 3, ---------- n - 1, by $\omega_1, \omega_2 --------------- \omega_p$.

Furthermore if ω represents one of the numbers $\alpha + \beta$, $\alpha - \beta$, $\alpha\beta$, each of the products $\omega\omega_1, \omega\omega_2 ---------- \omega\omega_p$ as can easily be seen, can be represented by the form,

(2) $h_1\omega_1 + h_2\omega_2 + ---------------- + h_p\omega_p$ having rational coefficients,

For example if we have $\omega = \alpha + \beta$ we would have the equation,

(3) $(\alpha + \beta)\alpha^\mu\beta^\nu = \alpha^{\mu+1}\beta^\nu + \alpha^\mu\beta^{\nu+1}$.

If $\mu < m - 1$, and $\nu < n - 1$, then both members of the equation belong to the series $\omega_1, \omega_2 ------------ -\omega_p$ and the form of equation (2) is satisfied.

If $\mu = m - 1$ and $\nu < n - 1$ then the first member of (3) may be represented by,

(4) $- A_1\alpha^{m-1}\beta^\nu - A\alpha^{m-2}\beta^\nu ------------ A_m\alpha\beta^\nu$.

Since (5) $\alpha^m + A_1\alpha^{m-1} + ----------------- + A_m = 0$

by hypothesis then, (4) is again of the form of equation (2).

If $\mu < m - 1$ and $\nu = n - 1$, then by noting also the identity

(6) $\quad \beta^n + B_1 \beta^{n-1} + \text{---------------} + B_n = 0.$

the desired form (2) may again be obtained. If finally $u = m - 1$ and $v = n - 1$, we may then consider the two identities (5) and (6) and again get the desired form (2).

In a similiar way we can prove that the same reasoning holds for $\alpha - \beta$, and $\alpha . \beta$. Hence in all these cases the following equations hold,

$$\omega\omega_1 = h_1' \omega_1 + h_2' \omega_2 + \text{------------} + h_p' \omega_p.$$
$$\omega\omega_2 = h_1'' \omega_1 + h_2'' \omega_2 + \text{-----------} + h_p'' \omega_p.$$

(7) --

--

$$\omega\omega_p = h_1^{(p)}\omega_1 + h_2^{p}\omega_2 + \text{---------------} + h_p^{(p)} \omega_p.$$

in which the coefficients are rational numbers. We may write (7) in the following form,

$$0 = (h_1' - \omega)\omega_1 + h_2'\omega_2 + \text{-------------} + h_p' \omega_p.$$
$$0 = h_1''\omega_1 + (h_1'' - \omega)\omega_2 + \text{-----------} + h_p'' \omega_p.$$

(8) $\text{--------------------------------------}$

$\text{---------- ----------------------------}$

$$0 = h_1^{(p)}\omega_1 + h_2^{(p)}\omega_2 + \text{---------------} + (h_p^{(p)} - \omega)\omega_p.$$

We have in (8) a set of p simultaneous equations in the p unknowns, $\omega_1, \omega_2, \text{------------} \omega_p$ and since $\alpha^0 \beta^0 = \omega_1 = 1$ (i.e.,not all the unknowns are equal to zero) then the following determinant is equal to zero,

(9) $\quad \begin{vmatrix} h - & h & \text{------------------}h \\ .h & h & \text{----------------}h \\ h & h & h - & \text{---------}h \\ \text{------------------------------} \\ h & h & h\text{------ -- } h - \end{vmatrix} = 0.$

This gives by developing in powers of ω the equation,

(10) $\omega^p + H_1 \omega^{p-1} + H_2 \omega^{p-2} - - - - - - + H_p = 0.$

in which H_1, H_2, H_3, ----------- H_p are rational integral

functions composed of h_1, h_2, h_3, --- ---- h_p, which are them-

selves rational numbers. Hence ω is an Algebraic Number.

To show α/β is an Algebraic number where $\beta \neq 0$, we

only need to divide the second of equations (1), through by

B_n and β^n. We thus obtain the following equation,

(11) $(1/\beta)^n + (B_{n-1}/ B_n)(1/\beta)^{n-1} + - - - - - - + (B_1 / B_n)(1/\beta) + (1/B) = 0.$

Hence $1/\beta$ is a root of the equation,

(12) $X^n + (B_{n-1}/ B_n)X^{n-1} + - - - - - - - - - - - (B_1 / B_n)X + (1/B_n) = 0.$

in which the coefficients are rational numbers. Proceeding

now as before we obtain α/β ,an algebraic number.

This theorem may also be proved in the following manner.

Let α be a root and α', α'' --------- $\alpha^{(n-1)}$ conjugate roots of

the equation,

(1) $X^n + p_1 X^{n-1} + p_2 X^{n-2} - - - - - - - - - - + p_n = 0.$

Let β be a root and β', β'' ---------- $\beta^{(m-1)}$ conjugate roots of

the equation,

(2) $X^m + q_1 X^{m-1} + q_2 X^{m-2} + - - - - - - - - - + q_m = 0.$

where p_1, p_2, ------ p_n, and q_1, q_2, -------q_m are rational num-

bers. Now forming the functions of α, α' --------- $\alpha^{(n-1)}$ and

β, β', β''---------------- $\beta^{(m-1)}$ we obtain,

$$f (\alpha , \beta) = \alpha + \beta = F_1 .$$

$$f_2 (\alpha, \beta') = \alpha + \beta' = F_2 .$$

$$f (\alpha, \beta'') = \alpha + \beta'' = F_3 ,$$

---------------------------- -

$$f(\alpha, \beta^{(m-1)}) = \alpha + \beta^{(m-1)} = F_m.$$

$$f(\alpha', \beta) = \alpha' + \beta = F_{m+1}$$

$$f(\alpha', \beta') = \alpha' + \beta' = F_{m+2}$$

---- ------

$$f(\alpha', \beta^{(m-1)}) = \alpha' + \beta^{(m-1)} = F_{2m}.$$

-------------------- -

$$f(\alpha^{(n-1)}, \beta^{(m-1)}) = \alpha^{n-1} + \beta^{m-1} = F_{mn}.$$

We wish to show that $\alpha + \beta$ is a root of the following equation,

(3) $\quad Z^{mn} + P_1 Z^{mn-1} + P_2 Z^{mn-2} + \text{------------} + P_{mn} = 0$.

Forming the equation having F_1, F_2, --------- F_{mn} as roots
we have,

(4) $\quad (Z - F_1)(Z - F_2)$ ---- ------------- $(Z - F_{mn}) = 0$.

We have, from the relation between the roots and coefficients,
the following equalities,

$$P_1 = -(F_1 + F_2 + F_3 + \text{-------------} + F_{mn})$$

$$P_2 = (F_1 F_2 + F_1 F_3 + F_2 F_3 + \text{------} + F_{mn-1} F_{mn})$$

$$P_3 = -(F_1 F_2 F_3 + F_1 F_3 F_4 + \text{-------} + F_{mn-2} F_{mn-1} F_{mn}.)$$

$$P_{mn} = (-1)^{mn} F_1 F_2 F_3 F_4 \text{-----} F_{mn}.$$

P_1, P_2, P_3, P_4, ------- P_{mn} are thus expressible in terms of the
symetric functions, $\alpha + \beta$, $\alpha + \beta'$, $\alpha + \beta''$, ------- $\alpha^{(n-1)} + \beta^{(m-1)}$,
which in turn are expressible in terms of the coefficients of
equation (1) and (2), that is, in terms of p_1, p_2, p_3, ----- p_n
and q_1, q_2, q_3, ------- q_m, since every rational integral funct-
ion of the roots of an algebraic equation can be expressed
rationally in terms of the coefficients.

Hence $\alpha + \beta$ satisfies equation (3), that is , $\alpha + \beta$ is an algebraic number. Similarily $\alpha - \beta$, $\alpha . \beta$, α / β can be shown to satisfy such an equation.

The following example illustrates the theorem, for n = 2 and m = 2. Let α and α' be the roots of the equation

$$X^2 + p_1 X + p_2 = 0 . \quad \text{and} \quad \beta \text{ and } \beta' \text{the roots of}$$

$$X^2 + q_1 X + q_2 = 0 .$$

$$F_1 = \alpha + \beta .$$

$$F_2 = \alpha' + \beta .$$

$$F_3 = \alpha + \beta' .$$

$$F_4 = \alpha' + \beta'$$

(1) $Z^4 + P_1 Z^3 + P_2 Z^2 + P_3 Z + P_4 = 0.$

$(Z - F_1) (Z - F_2) (Z - F_3) (Z - F_4) = 0 .$

$- P_1 = F_1 + F_2 + F_3 + F_4 .$

$= 2 (\alpha + \alpha' + \beta + \beta') = - 2p_1 - 2q_1 = - 2(p_1 + q_1)$

$P_2 = F_1 F_2 + F_1 F_3 + F_1 F_4 + F_2 F_3 + F_2 F_4 + F_3 F_4 .$

$= (\alpha + \alpha')^2 + (\beta + \beta')^2 + 2\alpha\alpha' + 2\beta\beta' + 3(\alpha + \alpha') (\beta + \beta') .$

$P_2 = p_1^2 + q_1^2 + 2(p_2 + q_2) + 3 p_1 q_1 .$

$- P_3 = F_1 F_2 F_3 + F_1 F_2 F_4 + F_2 F_3 F_4 + F_1 F_3 F_4$

$$= \left[(\beta + \beta')^2 (- \alpha - \alpha') + (\alpha + \alpha')^2 (-\beta - \beta'^2) + 2 \left\{ - (\beta + \beta') (\beta\beta') + (- (\alpha + \alpha')\alpha'\alpha) \right\} + 2 \left\{ - (\beta + \beta') (\alpha\alpha') + \beta\beta'(- \alpha - \alpha') \right\} \right]$$

$P_3 = q_1^2 p_1 + p_1^2 q_1 + 2 (q_1 q_2 + p_1 p_2) + 2 (q_1 p_2 + q_2 p_1)$

$P_4 = F_1 F_2 F_3 F_4 .$

$$= - (\alpha + \alpha') \left\{ - \beta\beta'(\alpha + \alpha') - \alpha\alpha'(\beta + \beta') - \beta\beta'(\beta + \beta') \right\} + (\alpha + \alpha')^2 + (\beta + \beta')^2 + \alpha\alpha'(\beta^2 + \beta'^2)$$

$P_4 = p_1 (q_2 p_1 + p_2 q_1 + q_1 q_2) + p_2^2 + p_2^2 + p_2 (q_1^2 - 2 q_2)$

Equation (1)above therefore becomes

(2) $Z^4 + 2(q_1 + p_1)Z^3 + \left\{ p_1^2 + 2(p_2 + q_2) + 3 p_1 q_1 + q_1^2 \right\} Z^2 + \left\{ q_1^2 p_1 \right.$

$p_1^2 q_1 + 2(q_1 q_2 + p_1 p_2) + 2(q_1 p_2 + q_2 p_1) \right\} Z + \left\{ p_1(q_2 p_1 + p_2 q_1 + q_1 q_2) \right.$

$\left. p_2^2 + q_2^2 + p_2(q_1^2 - 2 q_2) \right\} = 0$.

For instance if, $X^2 + 2 X + 1 = 0$. $\quad X = -1, -1 \quad \alpha = -1,$
$\alpha' = -1.$

and $X^2 + 3 X + 2 = 0.$ $\quad X = -2, -1.$ $\quad \beta = -2 \quad \beta' = -1.$

Equation (2) becomes,

$$Z^4 + 10 Z^3 + 37 Z^2 + 60 Z + 36 = 0.$$

$Z = -2$ or -3 satisfies the last equation for $\alpha + \beta = -3$

and $\alpha' + \beta' = -2.$

Theorem II .- If ω is a root of an algebraic equation,

whose coefficients are algebraic numbers, then ω is an alg-
ebraic number.

Let ω be a root of the equation

$\quad \omega^n + \alpha \, \omega^{n-1} + \beta \, \omega^{n-2} + \cdots \cdots \cdots \cdots \nu = 0.$

where α β ----------ν satisfy the following equations, having

rational coefficients,

$\quad \alpha^a + A_1 \alpha^{a-1} + \text{---------------} A_a = 0.$
$\quad \beta^b + B_1 \beta^{b-1} + \text{---------------} B_b = 0.$

$\text{--------------------------------}$

$\quad \gamma^c + C_1 \gamma^{c-1} + \text{---------------} C_c = 0$.

We will let p represent the product nab ----c and $\omega_1, \omega_2 \text{-----} \omega_p$
the numbers obtained by taking $\omega^{n'} \alpha^{a'} \beta^{b'} \text{-----------} \nu^{c'}$ where

$\quad n' = 0, 1, 2, \text{-------------} n - 1$

$\quad a' == 0, 1, 2, \text{-------------} a - 1$

$\quad b' = 0, 1, 2, \text{----------} b - 1$

$\text{-----------------------------------}$

$\quad c' = 0, 1, 2, \text{---------} c - 1$

Now if we form the products $\omega\omega_1, \quad \omega \omega_2 \text{----------------------} \omega \omega_p$.

each of the products, by using the set of identities given
above, can be reduced to the form

$$h_1\omega_1 + h_2\omega_2 + h_3\omega_3 + \text{-----------} + h_p\omega_p$$

where $h_1, h_2, h_3, \text{-----------} h_p$, are rational numbers, being
quantities arising from addition, subtraction and multiplication
of the coefficients $A_1, A_2, \text{------} A_a, B_1, B_2, B_3, \text{-------} B_b \text{---}$
$\text{----} C_1, C_2, C_3, \text{--------} C_c$. Proceeding as in theorem I, we
obtain p equations which reduce again to the form

$$\omega^p + H_1\omega^{p-1} + H_2\omega^{p-2} + \text{------------} + H_p = 0.$$

where $H_1, H_2, \text{------} H_p$ are rational integral functions of the
rational numbers $h_1, h_2, h_3, h_4 \text{----------} h_p$. Hence ω is an
algebraic number.

Definition.- By the norm of a number we mean the product
obtained by multiplying a number into its conjugates. If α'
is the conjugate of α then $N(\alpha) = (\alpha\alpha')$.

Theorem III. - If α is an arbitrary algebraic integer
and β is an algebraic integer diferent from zero, then two
integral numbers γ and v can always be so choosen that,

$$\alpha = v\beta + \gamma \qquad \text{and} \qquad (N(\gamma) \leftarrow N)(\beta)$$

Since the quotient of the two numbers is a number ω_1,
belonging to the field, K ., then we can write $\alpha/\beta = v + \omega_1$
or $\alpha = \beta v + \beta\omega_1$ where v is an integral number and $(N)\omega_1 < 1$.
From this it follows that the number $\gamma = \beta\omega_1 = \alpha - v\beta$ is
an integral number

Hence we have (1) $N(\gamma) = N(\beta, \omega_1)$
But the norm of the product of two numbers is equal to the pro-
duct of the norms as can easily be shown. Equation (1) may
hence be written $N(\gamma) = N(\beta) N(\omega_1)$

But $N(\omega_1) < 1$. Hence $N(\gamma) < N(\beta)$.

Definitions. - If we are operating in the domain R (1) i.e ,the domain of rational numbers, a set of quantities ω_1, ω_2 --------- ω_n in that domain, are said to be linearly independent if the equation,

$$\beta_1\omega_1 + \beta_2\omega_2 + \text{-----------} + \beta_n\omega_n = 0.$$

is true for no other values of β_1, β_2 ------------ β_n, except $\beta_1 = \beta_2 = \beta_3 = \beta_4 = \beta_5 = \text{----------} = \beta_n = 0$.   Otherwise the quantities are said to be linearly dependent.

A number field, or domain is said to be of degree n if it contains n independent numbers ω_1, ω_2 --------- ω_n with regard to R (1), but each n + 1 of its numbers with regard to R (1) are dependent.

From this definition it follows that between every number ξ of the field and the n numbers $\omega_1, \omega_2,$ --------- ω_n there exists the fo`llowing relation,

$$\beta\xi + \beta_1\omega_1 + \beta_2\omega_2 + \text{-----------------} + \beta_n\omega_n = 0.$$

where $\beta, \beta_1, \beta_2, \beta_3$ ------------ β_n belong to the domain R (1)

Since the n+1   numbers $\xi, \omega_1, \omega_2,$ ----------- ω_n are dependent, then β cannot be zero.   From which the following theorem results.

Theorem V- Every number ξ of the field K   can be represented by the equation,

$$\xi = r_1\omega_1 + r_2\omega_2 + r_3\omega_3 + \text{--------------} r_n\omega_n.$$

where $r_1, r_2, r_3,$ ------ r_n belong to R (1).

The numbers ω_1, ω_2 ----------- ω_n are called a base of the field. Theorem. V - An infinite number of bases can be choosen to represent any arbitrary number ξ in the field K .

From theorem IV we can write the following relations,

$$\omega_1' = r_1'\omega_1 + r_2'\omega_2 + \text{---------------} + r_n'\omega_n$$

$$\omega_2' = r_1''\omega_1 + r_2''\omega_2 + \text{-----------------} r_n''\omega_n.$$

$$\text{-------------------------------}$$

$$\text{-------------------------------}$$

$$\omega_n' = r_1^{(n)}\omega_1 + r_2^{(n)}\omega_2 + \text{---------------} r_n^{(n)}\omega_n.$$

where $\omega_1', \omega_2', \omega_3'$ ----------------- ω_n' are numbers in the field and $r_i^{(h)} \neq 0$. h = 1, 2, 3. ------ n. i = 1, 2 --------- n .

There are an infinite number of ways in which we can choose the following determinant, $D \neq 0$.

$$\begin{vmatrix} r_1', & r_2', & r_3', & \text{-------------------} & r_n' \\ r_1'', & r_2'', & r_3'', & \text{-------------------} & r_n'' \\ r_1''', & r_2''', & r_3''', & \text{-------------------} & r_n''' \\ \text{---------------------------------} \\ r_1^{(n)}, & r_2^{(n)}, & r_3^{(n)}, & \text{-------------------} & r_n^{(n)} \end{vmatrix} \neq 0.$$

Since we can choose $r_i^{(h)}$ in an infinite number of ways so that $D \neq 0$, it thus follows that the numbers $\omega_1', \omega_2',$ ------------ ω_n' can be choosen in an infinite number of ways. Therefore the number ξ can be represented in an infinite number of ways by the numbers $\omega_1', \omega_2' \omega_3'$ ------------------- ω_n' .

As an example we can consider the complex numbers. Let

$$\omega_1 = 1 \qquad \omega_2 = i .$$

then $\omega_1' = r_1'.1 + r_2'.i$.

$$\omega_2' = r_1''.1 + r_2''.i .$$

The r's in the determinant

$$\begin{vmatrix} r_1' & r_2' \\ r_1'' & r_2'' \end{vmatrix}$$

can be choosen in an infinite number of ways so that $D \neq 0$.

Taking
$$D = \begin{vmatrix} 2 & 3 \\ 3 & 4 \end{vmatrix}$$
we get
$$\omega_1' = 2 + 3 i$$
$$\omega_2' = 3 + 4 i.$$

If we wish to express any arbitrary number such as $4 + 5i$ with ω_1' and ω_2' as a base we would have,

$$4 + 5i = X (2 + 3i) + Y (3 + 4i).$$
$$2X + 3Y = 4$$
$$3X + 4Y = 5$$
$$X = -1. \quad Y = 2.$$
$$4 + 5i = -(2 + 3i) + 2(3 + 4i).$$

CHAPTER III.

QUADRATIC NUMBERS.

All numbers of the domain $\sqrt{m}$ are of the form $\dfrac{a + b\sqrt{m}}{c}$ a, b, and c being rational integers or zero. If m is a positive number then the domain contains only real numbers and is called a Real Domain. If m is negative then all the numbers of the domain of the form $\dfrac{a + b\sqrt{m}}{c}$ are imaginary in case $b \neq 0$, and the domain is called an Imaginary Domain.

To each number $\alpha = \dfrac{a + b\sqrt{m}}{c}$, belongs its conjugate $\alpha' = \dfrac{a - b\sqrt{m}}{c}$, such that α and α' satisfy the same quadratic equation with rational coefficients .

We will now investigate the value which c must have in order that $\alpha = \dfrac{a + b\sqrt{m}}{c}$, be a quadratic integer. Let $\alpha = \dfrac{a + b\sqrt{m}}{c}$, and $\alpha' = \dfrac{a - b\sqrt{m}}{c}$, where a, b , and c are relatively prime, be the roots of a quadratic equation,

$$(1) \quad X^2 + p_1 X + p_2 = 0.$$

then $p_1 = -(\alpha + \alpha') = -2a/c$ and $p = \alpha\alpha' = \dfrac{a^2 - b^2 m}{c^2}$ Hence equation (1) becomes,

$$(2) \quad X^2 - \frac{2a}{c} X + \frac{a^2 - b^2 m}{c^2} = 0.$$

In order that α be a quadratic integer, it follows from definition, that $\dfrac{2a}{c}$ and $\dfrac{a^2 - b^2 m}{c^2}$ must be rational integers. Suppose c is a prime, $p > 2$. Since $\dfrac{2a}{c}$ is an integer, then a must contain the factor p. Also $c^2 = p^2$ must be a factor of $a^2 - b^2 m$. But a^2 is divisible by p^2, hence $b^2 m$ must be divisible by p^2. But m, by hypothesis, contains no quadratic factor, hence b^2 must be divisible by p^2, that is , b is divisible by p. We thus have a , b , and c all containing a com-

mon factor p, which is contrary to the hypothesis that a , b, and c are relatively prime. Hence c cannot contain a prime factor greater than 2. c must therefore be equal to 2 or some power of 2. It can be shown in a way similar to the above that c cannot contain a higher power of 2 than the first. Hence α is of the form $\dfrac{a \; + \; b\sqrt{m}}{2}$, c however may equal 1

Theorem I.-Every quadratic integer is of the form

(1) $a + b \dfrac{(1+\sqrt{m})}{2}$ in case $m \equiv 1$ (modulus 4), or

(2) $a + b\sqrt{m}$ in case $m \equiv 2$ or 3 (modulus 4). where a and b are any rational integers.

(1) If $m \equiv 1$ (mod. 4) and a and b are rational integral numbers, then the number . $\alpha = \dfrac{a + b\sqrt{m}}{2}$ is integral if $2a/2$ and $\dfrac{a^2 + b^2 m}{4}$ are integral. It is evident that $2a/2$ is an integer, $\dfrac{a^2 - b^2 m}{4}$ is integral if $a^2 - b^2 m$ is divisible by 4 . Two cases arise which fulfill this condition. Either a and b can both be even or a and b can both be odd. In the first case, $\alpha = \dfrac{a + b\sqrt{m}}{2} = (2a_1 \; \underline{+} \; \dfrac{2b\sqrt{m}}{2} = a_1 + b_1\sqrt{m}$

In the second case,

$$= \dfrac{a + b\sqrt{m}}{2} = \dfrac{(2a_1 + 1) + 2 \; b_1 + 1\sqrt{m}}{2} = a_2 + b_2 \dfrac{(1+\sqrt{m})}{2}$$

In both cases we see that the integral numbers are included in the expression $a + b \dfrac{(1 + \sqrt{m})}{2}$.

(2) If $m \equiv 2$ (mod. 4), or $m \equiv 3$ (mod. 4) then the number

$\alpha = \dfrac{a \; + \; b\sqrt{m}}{2}$ is integral if $a^2 - b^2 m$ is divisible by 4. Since the square of an integral number is always congruent to 0 or 1, modulus 4, according as the number is even or odd, it follows that a and b must both be even. Hence all the integral numbers are of the form $a + b\sqrt{m}$.

It is convenient to represent all integral numbers by
$a + b\omega$ where $\omega = \dfrac{1 + \sqrt{m}}{2}$ when $m \equiv 1$ (mod. 4) and $\omega = \sqrt{m}$,
when $m \not\equiv 1$ (mod. 4). 1 and ω represent a base of the domain.

By the Discriminant of a number we mean the square of the
difference between a number α and its conjugate α' i. e., $d(\alpha) = (\alpha - \alpha')^2$. The discriminant of the field $k\sqrt{m}$ is $d(\omega) = (\omega - \omega')^2$

Example.- Let the field be $k\sqrt{-2}$. $m = -2$, $m \equiv 2$ (mod.4)
land $\omega = \sqrt{-2}$ represent a base of the field.

All the integral numbers are of the form $a + b\sqrt{-2}$.

To every number $\alpha = a + b\sqrt{-2}$, belongs its conjugate $\alpha = a - b\sqrt{-2}$

The norm of $\alpha = (\alpha\alpha') = a^2 + 2b^2$.

The discriminant of an integral number α of the field is
$d(\alpha) = (\alpha - \alpha')^2 = -8 b^2$. The discriminant of the field is
$d(\omega) = (\omega - \omega')^2 = -8$

As another base of the field we may use $\omega_1 = 3 \pm 4\sqrt{-2}$, and
$\omega_2 = 2 + 3\sqrt{-2}$

We will now consider Lagrange's Theorem in regard to
quadratic numbers.

Theorem.II.- Every irrational quadratic number can be developed intoa periodic continued fraction, and vice versa.

In order to prove this theorem we will first establish
the following lema.

Lema.- If we have given a quadratic equation with integral
coefficients,
$\quad$ (1) $aX^2 + bX + c = 0$ $\quad$ and place

$\quad\quad$ $X = m + 1/y$, where m is an integer, then
the above equation reduces to a quadratic equation in y, having integral coefficients

$\qquad$ (2) $\ a'Y^2 + b'Y + c' = 0.$, $\qquad$ with the same discriminant

as the given equation, that is,

$$b'^2 - 4\,a'\,c' = b^2 - 4\,a\,c\ .$$

$\qquad$ Replacing X in the given equation by $\ m + 1/Y$ we get,

$\qquad$ $a\ (\ m + 1/Y)^2 + b\ (\ m + 1/Y) + c = 0.\ $,or

(3) $\ \ (\ a\,m^2 + bm + c)Y^2 + (2am + b)Y + a = 0.$ which is an equa-

tion having integral coefficients. $\quad$ Equating coefficients

in (2) and (3) we get,

$$am^2 + bm + c = a'\,.$$
$$2am + b = b'\,.$$
$$a = c'\,.$$

From these equations we get,

$\qquad$ $b'^2 - 4a'c' = (2am + b)^2 - 4a(am^2 + bm + c).$

$\qquad$ $b'^2 - 4a'c' = 4a^2m^2 + 4abm + b^2 - 4a^2m^2 - 4abm - 4ac\ .$

$\qquad$ $b'^2 - 4a'c' = b^2 - 4ac\ .$

Thus if we have $\ 5X^2 + 7X + 1 = 0\ .$

$$X = \frac{-7 \pm \sqrt{49 - 20}}{10} = \frac{-7 \pm \sqrt{29}}{10.}$$

$\qquad$ Hence $\qquad X = 1 + 1/Y\ .$

$$5(1 + 1/Y)^2 + 7(1 + 1/Y) + 1 = 0.$$

$$13Y^2 + 17Y + 5 = 0\quad .$$

$$Y = \frac{-17 \pm \sqrt{29}}{26}$$

$\qquad$ By means of this lema we can now show that one positive

root of a quadratic equation can be developed into a periodi-

ic continued fraction. $\quad$ We can always reduce a quadratic eq-

uation which does not have a multiple root , by means of the

above transformation, to an equation having one positive root.

For by properly choosing m we can make 1/Y equal to a positive

fraction and hence $\ Y > 1\ .$

We will thus consider an equation,

$aX^2 + bX + c = 0$.   in which a and c are of opposite sign.
Let m_1 be the integral part of the positive root.   We may
then place $X = m_1 + 1/X_1$, in the above equation and obtain
a quadratic equation in X_1

$$a_1X_1^2 + b_1X_1 + c_1 = 0 .$$

which has a single positive root and consequently a_1 and c_1 are
of opposite sign.   Let m_2 be the integral part of the posi-
tive root of this equation.   We may then place,

$$X_1 = m_2 + 1/X_2 \text{ and obtain for } X_2$$

$a_2X_2^2 + b_2X_2 + c_2 = 0$. having again a single positive
root and hence a_2 and c_2 again differ in sign.   Continuing
this process we obtain,

$$a_3X_3^2 + b_3X_3 + c_3 = 0 \cdot\cdot$$
$$a_4X_4^2 + b_4X_4 + c_4 = 0 .$$

$$------------$$

$$------------$$

In all these equations the following relation holds,

(4) $b^2 - 4ac = b_1^2 - 4a_1c_1 = b_2^2 - 4a_2c_2 = \text{-------------------}$

Furthermore since the a's and c's differ in sign

(5) $ac < 0,$ $a_1c_1 < 0,$ $a_2c_2 < 0,$ -----------------

We will represent the equations given above by the general
equation,

$AX^2 + BX + C = 0 .$

The number of such equations satisfying the above conditions
is limited. For if we call Δ the common value of the quanti-
ties in (4) we have

$$B^2 - 4AC = \Delta \text{ and } AC < 0 .$$

We thus have $\quad B^2 = \triangle + 4AC$

$\qquad$ Hence $B^2 < \triangle$ and $\quad |B| < \sqrt{\triangle}$

If λ is the greatest integer contained in $\sqrt{\triangle}$, the number B cannot have any other values except,

$$0 \pm 1 \pm 2 \pm 3 \pm \text{-------------------} \pm \lambda.$$

To values determined for B, must correspond values for A and C, and the system of values must satisfiy these conditions,

$$AC = \frac{B^2 - \triangle}{4}$$

The number of values for this system is thus limited. Since the number of these equations , satisfying the indicated conditions is limited, the incomplete quotients, which are the positive roots of the equations are thus limited in number. Hence in the reduction of X to a continued fraction , we arrive finally to an incomplete quotient, determined by an equation identical to that which defined a preceeding incomplete quotient. It is evident that, by a repetition of the process the same incomplete quotients will again be reproduced . The quadratic number will therefore be developed into a periodic continued fraction.

Example.- $\quad$ (1) $\quad 9X^2 - 13X + 3 = 0.$

$$X = \frac{13 \pm \sqrt{61}}{18}$$

$$X = 1 + 1/X_1$$

$$9X_1^2 + 18X_1 + 9 - 13X_1^2 - 13X_1 + 3X_1^2 = 0.$$

$\qquad$ (2) $\quad X_1^2 - 5X_1 - 9 = 0 .$

$$X_1 = \frac{5 \pm \sqrt{61}}{2}$$

$$X_1 = 6 + 1/X_2$$

$$36X_2^2 + 12X_2 + 1 - 30X_2^2 - 5X_2 - 9X_2^2 = 0 .$$

$\qquad$ (3) $\quad 3X_2^2 - 7X_2 - 1 = 0 .$

$$X_2 = \frac{7 \pm \sqrt{61}}{6}$$

$$X_2 = 2 + 1/X_3$$

$$12X_3^2 + 12X_3 + 3 - 14X_3^2 - 7X_3 - X_3^2 = 0 \ .$$

$$(4) \quad 3X_3^2 - 5X_3 - 3 = 0 \ .$$

$$X_3 = \frac{5 \pm \sqrt{61}}{6}$$

$$X_3 = 2 + 1/X_4$$

$$12X_4^2 + 12X_4 + 3 - 10X_4^2 - 5X_4 - 3X_4^2 = 0 \ .$$

$$(5) \quad X_4^2 - 7X_4 - 3 = 0 \ .$$

$$X_4 = \frac{7 \pm \sqrt{61}}{12}$$

$$X_4 = 7 + 1/X_5$$

$$49X_5^2 + 14X_5 + 1 - 49X_5^2 - 7X_5 - 3X_5^2 = 0 \ ,$$

$$(6) \quad 3X_5^2 - 7X_5 - 1 = 0 \ .$$

Equation (6) is the same as equation (3), hence any further development will only repeat the incomplete quotients arising from equations (3) (4) and (5) . The periodic continued fraction hence becomes,

$$X = 1 + \frac{1}{6+} \ \frac{1}{2} + \ \frac{1}{2} + \ \frac{1}{7} + \ \frac{1}{2} + \ \frac{1}{2} + \ \frac{1}{7} + \ \text{----------}$$

We will now prove the converse of the above theorem Theorem III. Every periodic continued fraction can be made the root of a quadratic equation.

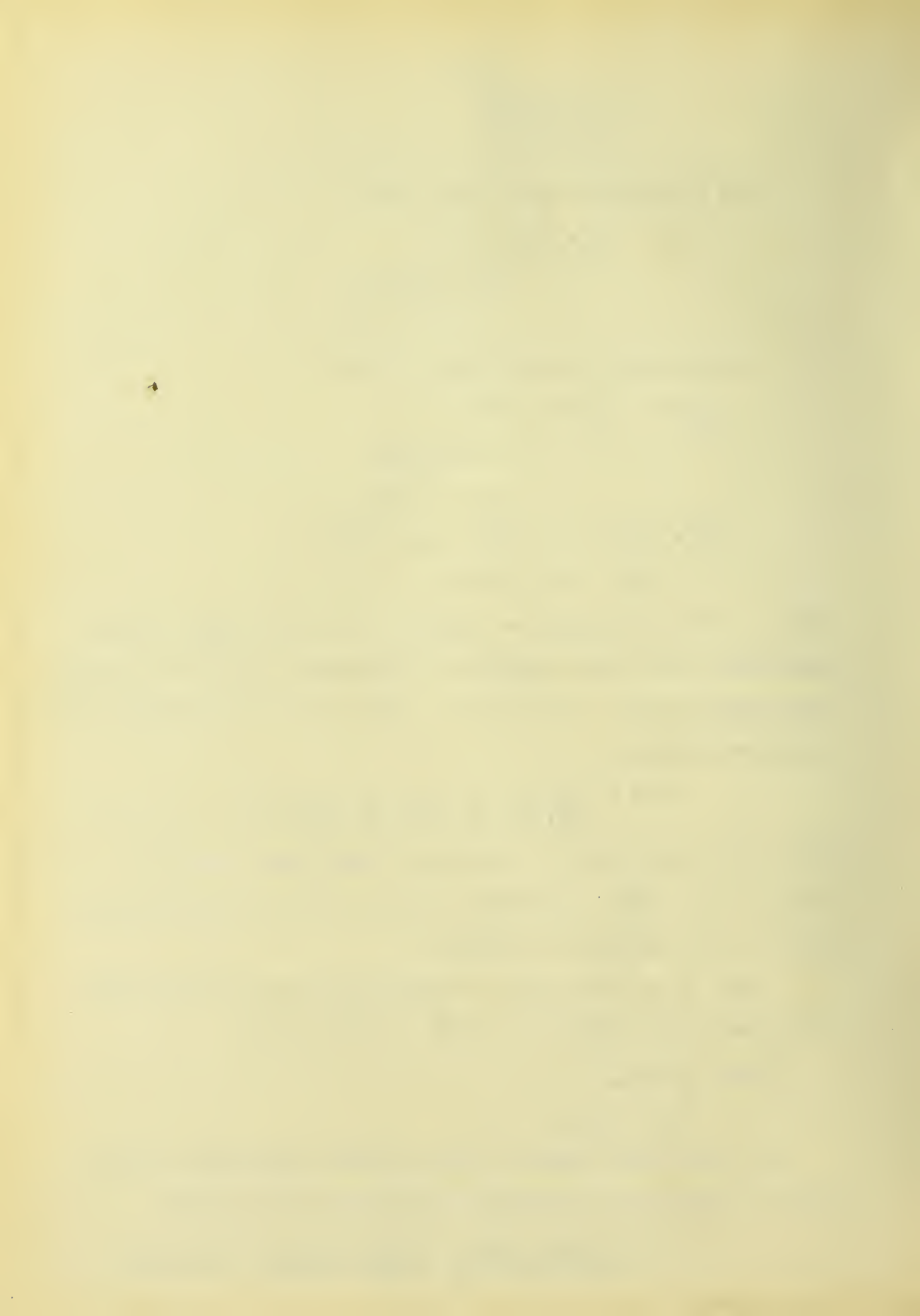Let a_k be the first incomplete quotient of the first period and h the number of terms of the period.

Then $a_k = a_{k+h}$

$$X_k = X_{k+h-1}$$

Let X be the value of the periodic continued fraction. From the property of continued fractions we may write,

$$X = \frac{P_{k-1} X_{k-1} + P_{k-2}}{Q_{k-1} X_{k-1} + Q_{k-2}} = \frac{P_{k+h-1} X_{k-1} + P_{k+h-2}}{Q_{k+h-1} X_{k-1} + Q_{k+h-2}}$$

where X_{K-1} is the value of the continued fraction from the P_{k-1}st

convergent on.   From the above relation we obtain,

$$(Q_{K-1}X - P_{K-1})X_{K-1} + Q_{K-2}X - P_{K-2} = 0 .$$

$$(Q_{K+h-1}X - P_{K+h-1})X_{K-1} + Q_{K+h-2}X - P_{K+h-2} = 0 .$$

Eliminating X_{K-1} from these equations, we obtain the following

quadratic equation in X

$$(1) (Q_{K-1} Q_{K+h-2} - Q_{K-2} Q_{K+h-1})X^2 - (Q_{K-1} P_{K+h-2} - Q_{K-2} P_{K+h-1} +$$

$$P_{K-1} Q_{K+h-2} - P_{K-2} Q_{K+h-1})X + P_{K-1} P_{K+h-2} - P_{K-2} P_{K+h-1} = 0 .$$

Since it is a property of continued fractions that the conver-

gents are alternately less and greater than the fraction, it

is evident that the above equation has one root between $\dfrac{P_{K-2}}{Q_{K-2}}$,

and $\dfrac{P_{K-1}}{Q_{K-1}}$.   Substituting these values for X give the foll-

owing results,

$$(-1)^K \frac{Q_{K+h-2}}{Q_{K-2}} \left(\frac{P_{K-2}}{Q_{K-2}} - \frac{P_{K+h-2}}{Q_{K+h-2}} \right) .$$

$$(-1) \frac{Q_{K+h-1}}{Q_{K-1}} \left(\frac{P_{K-1}}{Q_{K-1}} - \frac{P_{K+h-1}}{Q_{K+h-1}} \right) .$$

which are opposite in sign.

It is this root which is equal to X .

Example.- Using the value of X we obtained in the previous

example for the periodic continued fraction we have,

$$X = 1 + \frac{1}{6} + \frac{1}{2} + \frac{1}{2} + \frac{1}{7} + \frac{1}{2} + \frac{1}{2} + \frac{1}{7} + \text{---------}$$

$$\frac{P_{K-2}}{Q_{K-2}} = \frac{1}{1} , \quad \frac{P_{K-1}}{Q_{K-1}} = \frac{7}{6} , \quad \frac{P_{K+h-2}}{Q_{K+h-2}} = \frac{37}{32} , \quad \frac{P_{K+h-1}}{Q_{K+h-1}} = \frac{274}{237} .$$

Substituting these values in equation (1) we get,

$$(6. 32 - 1. 237)X^2 - (6. 37 - 1. 274 + 7. 32 - 1. 237)X +$$

$$- (7. 37 - 1. 274) = 0 .$$

or $- 45X^2 + 65X - 15 = 0 .$

  i.e., $9X^2 - 13X + 3 = 0 .$

which is the original equation, having X as a root.

Divisibility of Integral Numbers.

The question arises in the system of algebraic numbers, as to the factoring of integral numbers. Can integral numbers be factored in only one way as in our ordinary number system or, are there some domains in which a number can be factored in more than one way? We will consider some examples and then draw our conclusions.

Suppose $\alpha = a_1 + a_2 \sqrt{-1}$ and $\beta = b_1 + b_2 \sqrt{-1}$ are any two numbers in the domain $\sqrt{-1}$, such that $N(\alpha) \overset{>}{=} N(\beta)$. Now by dividing α by β we will obtain an integral number and a remainder which we will take as the smallest remainder,

$$\alpha/\beta = \alpha \beta' / N(\beta) = \gamma + \frac{r + s\sqrt{-1}}{N(\beta)}$$

In the remainder $\frac{r + s\sqrt{-1}}{N(\beta)}$, r and s may lie between 0 and $-N(\beta)$, or $-1/2 N(\beta)$ and $+1/2 N(\beta)$. Hence r and s must be so choosen that $|r| \overset{<}{=} 1/2 N(\beta)$ and $|s| \overset{<}{=} 1/2 N(\beta)$. Now if we place $\rho_0 = \frac{r + s\sqrt{-1}}{(\beta')}$
then $\alpha = \beta\gamma + \rho_0$, and $N(\rho_0) = \frac{r_2 + s_2}{N((\beta'))}$, $\overset{<}{=}$
$$\frac{\frac{1}{4} N(\beta)^2 + \frac{1}{4} N(\beta)^2}{N(\beta')} \overset{<}{=} \frac{1}{2} N(\beta)$$

If $N(\rho_0) > 1$ then we can divide β by ρ_0 and hence $\beta = \gamma_1 \rho_0 + \rho_1$, in which ρ_1 is to be choosen so that $N(\rho_1) \overset{<}{=} \frac{1}{2} N(\rho_0)$. This division may be continued until we obtain $N(\rho_{n-1}) > 1$ and either, $N(\rho_n) = 0$ or, $N(\rho_n) = 1$. One of these last possibilities must happen since the norms of the remainders represent a converging series of rational integral numbers. In the case where $N(\rho_n) = 0$, α and β are divisible by ρ_{n-1} and in the case where $N(\rho_n) = 1$, ρ_n is contained in 1, and α and β are divisible by 1 or a number divisible by 1 and

thus relatively prime. Hence the integral numbers of the domain $\sqrt{-1}$ can be separated into their prime factors in only one way.

Now if we consider the general case where we have the domain $\sqrt{m}$ $m \not\equiv 1$ (Modulus 4), and with the same conditions as above $\dfrac{\alpha}{\beta} = \dfrac{\alpha \cdot \beta'}{N(\beta)} = \gamma + \dfrac{r + s\sqrt{m}}{N(\beta)}$.

or $\alpha = \gamma \beta + \rho_0$

where again $|r| < \frac{1}{2} \; |N(\beta)|$ and $|s| \leq \frac{1}{2} \; |N(\beta)|$

Then $N(\rho_0) = \dfrac{r^2 - s^2 m}{N(\beta')} \leq \dfrac{\frac{1}{4} N(\beta)^2 - \frac{1}{4} N(\beta)^2 m}{N(\beta)} \leq N(\beta)\left|\frac{1}{4} - \frac{m}{4}\right|$

From this inequality it follows that $\left|N(\rho_0)\right| < \left|N(\beta)\right|$ if $3 > m > -3$

In case $\left|N(\rho_0)\right| > \left|N(\beta)\right|$ we cannot reduce the remainders to a converging series and hence we cannot say that there is only one way of separating the integral numbers of the domain $\sqrt{m}$ into their prime factors.

If $m \equiv 1$ (Modulus 4) the same result can be obtained in a similar way.

CHAPTER IV.

Ideals in The Quadratic Domain.

An Ideal of a Domain of Rationality is a system of integers of the domain, such that any linear division of the numbers of the system belong to the system, or otherwise expressed. If we have a system of integral numbers of the field $K \sqrt{m}$, namely $1 = (\alpha , \beta , \gamma , ---------)$, of such a nature that every linear combination $\alpha \lambda + \beta \mu + \gamma \nu + ---------$, of the numbers $\alpha , \beta , \gamma , ------$, with the integral numbers $\lambda , \mu , \nu , -----$ of the field, gives numbers again of the system, and all the numbers of the system can be obtained in this way, then the system is called an Ideal of the Field.

If every integer of the system is a multiple of a single integer, the ideal is called a Principal Ideal.

Definitions- Two ideals $(\alpha , \beta , \gamma , ---------)$ and $(\alpha_1 , \beta_1 , \gamma_1 , ---------)$ are equal, that is,

$$(\alpha , \beta , \gamma , ---------) = (\alpha_1 , \beta_1 , \gamma_1 , -----------)$$

if each of the numbers $\alpha , \beta , \gamma , ---------$, of the first ideal belongs also to the second ideal (i.e., can be expressed by a linear combination $\alpha_1 \lambda + \beta_1 \mu + ------------$) and vice versa, if every number $\alpha_1 , \beta_1 , \gamma_1 , ---------$ of the second ideal belongs to the first ideal.

By the product of two ideals, we shall understand the following:- Having given two ideals of the field $K \sqrt{m}$

$$I_1 = (\alpha , \beta , \gamma , ---------------)$$
$$I_2 = (\alpha_1 , \beta_1 , \gamma_1 , ---------------),$$

then their product is the ideal which is composed of all the numbers which we obtain by multiplying every number of I_1 by

every number of I_2 and adding to this system all linear com-
binations of this product with the integral numbers of the field.

An ideal I_1 is said to be divisible by I_2, if a third
ideal I_3 of the domain can be found such that

$$I_1 = I_2 I_3 .$$

I_3 is called the quotient of the ideals I_1 and I_2.

Any ideal involving unity has only one divisor in any do-
main of rationality.

We speak of The Greatest Common Divisor of two ideals
as being the smallest ideal which contains both of the ideals.
Symbolically we indicate it thus:-

$$I_1 + I_2 \equiv \text{G. C. D. of } I_1 \text{ and } I_2 .$$

By The Least Common Multiple of two ideals we mean the
ideal composed of the numbers common to both ideals. It is in-
dicated thus:- $I_1 - I_2 = \text{L. C. M.}$ of I_1 and I_2.

When we compare ideals it must always be done in the same
domain of rationality.

Theorem I.- In every ideal of the field $K\sqrt{m}$ there are always
two integral numbers i_1 and i_2 of the field, of such a nature that every
number of the ideal can be represented by a linear combination
of these two numb ers with rational integral coefficients,

$$l_1 i_1 + l_2 i_2 .$$

Expressing each number of the field with 1 and ω as a base
we have $I = (a + b\omega , \ a_1 + b_1\omega , \ a_2 + b_2\omega \text{---------------})$
Now we wish to show that if $a + b\omega$ and $a_1 + b_1\omega$, are any two
numbers of the ideal, then $a' + b'\omega$ is also a number of the
ideal, where b' is the greatest common divisor of b and b_1.
If x and y are rational integers, then from the definition of
an ideal we know that $x(a + b\omega) + y(a_1 + b_1\omega)$ belongs to the

ideal. We can always choose x and y so that the following
equation is satisfied:-

$$xb + yb_1 = b'$$

Hence $a' + b'\omega$ is a number of the ideal. We can repeat this
process with $a' + b'\omega$ and $a_2 + b_2\omega$ and so on with every num-
ber of the ideal. Thus we see that the ideal contains a num-
$J_1 + i_2\omega$ in which i_2 is the greatest common divisor of b, b_1,
b_2,------ while J_1 is a rational integral number, which is yet
to be determined.

The numbers $\dfrac{b}{i_2}$, $\dfrac{b_1}{i_2}$, $\dfrac{b_2}{i_2}$, -----------are rational integral
numbers. Hence it follows that the rational integral numbers,

$$a + b\omega - \frac{b}{i_2}(J_1 + i_2\omega) = a - \frac{b}{i_2}J_1$$
$$a_1 + b_1\omega - \frac{b_1}{i_2}(J_1 + i_2\omega) = a_1 - \frac{b_1}{i_2}J_1$$

----

all belong to the ideal. Consequently it follows that every
ideal contains an arbitrary number of rational integral num-
bers. Now let i be the greatest common divisor of all the
rational integral numbers of the ideal. If we now choose
a rational integral number, v, such that,

$$0 \leqq i_1 = J - vi < i$$

then $J - iv + i_2\omega = i_1 + i_2\omega$ is also a number of the ideal and

$$i_1 = i, \qquad i_2 = i_1 + i_2\omega.$$

which are the numbers of the desired nature.

Let $\alpha = a + b\omega$ be any arbitrary number of the ideal, then
$l_2 = \dfrac{b}{i_2}$ is integral and the number $\alpha - l_2 i_2 = a - l_2 i$, which is
a rational integer, belongs also to the ideal. Hence according
to our definition of i we have,

$$a - l_2 i_1 = l_1 i,$$ where l_1 is a rational integer.

From the last two equations we thus get,

$$\angle = l_1 i + l_2 i_2 = l_1 i_1 + l_2 i_2.$$

From this it follows that the ideal can be represented by the form $I = (i, i_1 + i_2 \omega)$ which is called the Cannonical Representation.

We will now investigate the relation existing between the rational numbers, i , i_1, i_2 of the ideal. If x and y are any two rational integers, then according to the definition of an ideal we may write the following relation,

$$xi\omega + y(i_1 + i_2 \omega) = \omega(xi + yi_2) + i_1 y.$$

which represents a number of the ideal.

Now since i_2 is the greatest common divisor of $xi + i_2 y$ we have,

$$xi + i_2 y \equiv 0 \ (\text{modulus } i_2)$$

But
$$i_2 y \equiv 0 \ (\text{modulus } i_2)$$

Hence
$$i \ x \equiv 0 \ (\text{modulus } i_2) \quad \text{i.e.,} \quad i \text{ is a multi-}$$
ple of i_2 .

Likewise $\omega'(i_1 + i_2 \omega) = i_1 \omega' + \omega \omega' i_2$ is a number of the ideal. Hence we see that i_1 is a multiple of i_2.

The numbers $i_1 = i$ and $i_2 = i_1 + i_2 \omega$, are called a Base of the Ideal.

In an infinite number of ways another base i_1^* , and i_2^* can be derived from the base i_1 , and i_2 .

$$i_1^* = a_1 i_1 + a_2 i_2 .$$

$$i_2^* = b_1 i_1 + b_2 i_2 .$$

a_1 , a_2, b_1, b_2 , being rational integers. In order for this to be true, we must have $a_1 b_2 - a_2 b_1 = \pm 1.$ Since this relation can be satisfied in an infinite numbers of ways, the above statement is therefore true.

The followingexamples illustrate the cannonical represent-
ation of ideals and show how the ideals (18) and (42) can
be factored in the domain $\sqrt{7}$.

Example 1. $18 = 2 \cdot 3^2 = (5 + \sqrt{7})(5 - \sqrt{7})$

From these factors we obtain the following ideals :-

$$(2,\ 5 + \sqrt{7}) = (2,\ 1 - \sqrt{7})$$
$$(2,\ 5 - \sqrt{7}) = (2,\ 1 - \sqrt{7}).$$
$$(3^2,\ 5 + \sqrt{7}) = (3^2,\ 5 + \sqrt{7}).$$
$$(3^2,\ 5 - 7) = (3^2,\ 5 - \sqrt{7}).$$

in which the right hand members are represented cannonically.
We have here ideals which represent the factors of 18.   Hence

$$(18) = (2,\ 1 - \sqrt{7})^2 (3^2,\ 5 + \sqrt{7})(3^2,\ 5 - \sqrt{7}).$$

$(2,\ 1 - 7) = (4,\ 2 - 2\ 7,\ 8 - 2\ 7) = (2)$

$(3^2,\ 5 + \sqrt{7})(3^2,\ 5 - \sqrt{7}) = (3^2,\ 3^2 \cdot 5 + 3^2 \cdot \sqrt{7},\ 3^2 \cdot 5 - 3^2 \cdot \sqrt{7},\ 18) = (3^2)$

Therefore $(18) = (2)(3^2)$.

Example 2. $42 = 6.7 = (7 + \sqrt{7})(7 - \sqrt{7})$.

The cannonical representation of the ideals formed from these
factors is: $(6,\ 7 + \sqrt{7}) = (6,\ 1 + \sqrt{7})$

$$(6,\ 7 - \sqrt{7}) = (6,\ 1 - \sqrt{7}).$$
$$(7,\ 7 + \sqrt{7}) = (7,\ \sqrt{7}).$$
$$(7,\ 7 - \sqrt{7}) = (7,\ \sqrt{7}).$$

As in example 1 we have again,

$$(42) = (7,\ \sqrt{7})^2 (6,\ 1 + \sqrt{7})(6,\ 1 - \sqrt{7}).$$

$$(7,\ \sqrt{7})^2 = (49,\ 14\sqrt{7},\ 7) = (7).$$

$(6,\ 1 + \sqrt{7})(6,\ 1 - \sqrt{7}) = (36,\ 6.1 + 6\sqrt{7},\ 6.1 - 6\sqrt{7},\ 6) = (6).$

Therefore $(42) = (6)(7)$.

Congruence with Respect to Ideals.

A number α is congruent to 0 modulus I, $\alpha \equiv 0(\text{mod. I})$, if α and I belong to the same domain and α appears in the ideal I .

$\alpha \equiv \beta$ (modulus I) if α, β and I belong to the same domain and $\alpha - \beta$ appears in the ideal I.

If α and $\alpha - \beta$ do not belong to the ideal I then

$\alpha \not\equiv 0$ (modulus I) and $\alpha \not\equiv \beta$ (modulus I)

Definitions.- If in the ideal $I_1 = (\alpha, \beta, \gamma, \text{--------------})$ we replace each number of I_1 by its conjugate, then the resulting ideal $I_1' = (\alpha', \beta', \gamma', \text{--------------})$ is called the Conjugate Ideal of I_1.

The Norm of an ideal I_1 is the product obtained by multiplying I_1 by its conjugate I_1'. i.e., $N(I_1) = I_1 I_1'$.

Theorem Il. - The number of distinct residues arising from all integral numbers which are incongruent to 0 modulus I, is equal to $N(I) = i\, i_2$ where $I = (i, i_1 + i_2\omega)$

We will represent by the equation,

$$a + b\omega \not\equiv 0 \text{ (mod. I.)}$$

all the incongruent numbers arising from all combinations of the following:-

(1)
$$a = 0, 1, 2, \text{-------} i - 1.$$
$$b = 0, 1, 2, \text{-------} i_2 - 1.$$

The system of integral numbers represented by all combinations of (1) comprises a set of $i\, i_2$ numbers, which are of such a nature that, 1st. No two can be congruent with respect to modulus 1. Hence the difference of any two numbers of the above system

$$a_k + b_k\omega - (a_{k'} + b_{k'}\omega)$$

is not contained in the ideal I.

Furthermore, 2nd· Any one number of the field is congruent to one and only one number of the field. Therefore since $a = 0, 1, 2, --------- i - 1.$, and $b = 0, 1, 2, -------- i_2 - 1.$ represents all the distinct residues with respect to i and i_2, then for a given number $A + B\omega$ of the field we can choose some number $a + b\omega$ from the above system, so that the following equation is satisfied:-

(2) $A + B\omega - (a + b\omega) = l_1 i + l_2 (i_1 + i_2 \omega)$.

where l_1 and l_2 are integral numbers. In order that equation 2 be true, we must choose a and b so that,

   $b \equiv B(\text{mod. } i_2), \quad \text{i.e.,} \quad B - b = l_2 i_2$

   $a \equiv A - l_2 i_1 (\text{mod. } i)$

Since $A + B\omega$ was any number of the field we thus have every number of the field congruent to one of the above numbers arising from the combinations of equation 1.

Hence the number of distinct residues arising from all integral numbers which are congruent to zero modulus I is equal to $i\, i_2$.

Example.- $I = (7, 4 + \sqrt{-5})$

In this ideal the number of the least set of residues is,

   $i\, i_2 = 7.1 = 7.$ The residues are 0, 1, 2, 3, 4, 5, 6.

Let $8 + 3\sqrt{-5}$ be any arbitrary number of the field. Then

   $8 + 3\sqrt{-5} - 3(4 + \sqrt{-5}) = -4.$ $7 - 4 = 3.$

Therefore $8 + 3\sqrt{-5} \equiv 3$ (modulus I).

The number $5 + 3\sqrt{-5}$ is a number of the ideal. For,

   $5 + 3\sqrt{-5} = 7x + y(4 + \sqrt{-5})$

   $7x + 4y = 5.$

         $y = 3, \quad x = -1.$ Hence x and y are integral.

Theorem III.- The product of an ideal and its conjugate ideal
is equal to a rational principal ideal. i.e., $1, I_I' = (\mathbb{N}(I))$.

$$\text{Let } \underset{(1)}{I_I} = (i, i_1 + i_2\omega)$$

$$I_I' = (i, i_1 + i_2\omega)$$

We have already shown that i and i_1 are multiples of i_2, i.e.,

$$i = a\, i_2, \quad i_1 = a_1 i_2.$$

Replacing i and i_1 in equation (1) by their values we get,

$$I_I = (ai_2, a_1 i_2 + i_2\omega) = (i_2)(a, a_1 - \omega)$$

$$I_I' = (ai_2, a_1 i_2 + i_2\omega') = (i_2)(a, a_1 + \omega').$$

Since a is the greatest common divisor of all the real numbers
in the ideals $(a, a_1 + \omega)$ and $(a, a_1 + \omega')$ we have the fol-
lowing congruence:- $(a_1 + \omega)(a_1 + \omega') \equiv 0 \pmod{a}$

Hence multiplying the two ideals we obtain,

$$I_I I_I' = (i_2)(a, a_1 + \omega)(i_2)(a, a_1 + \omega')$$

$$I_I I_I' = (i_2^2)(a^2, aa_1 + a\omega, aa_1 + a\omega', (a_1 + \omega)(a_1 + \omega')).$$

We will now show that the second member of this product is equal
to the principal ideal (a). In order to do this we will take the
field having $\sqrt{m}$ as a parameter and consider three cases.

Case 1. $m \equiv 3 \pmod{4}$. $\omega = \sqrt{m}$, $\omega' = -\sqrt{m}$.

In this case we obtain the following equations:-

$$(a^2, aa_1 + a\omega, aa_1 + a\omega', (a_1 + \omega)(a_1 + \omega')) =$$

$$(a^2, aa_1 + a\sqrt{m}, aa_1 - a\sqrt{m}, a_1^2 - m) =$$

$$(a^2, 2aa_1, 2a\sqrt{m}, 2am, a_1^2 - m) =$$

$$(a)(a, 2m, \frac{a_1^2 - m}{a}, 2a_1, 2\sqrt{m}). \text{ a being the highest common}$$

factor in this last equation.

We shall now prove that,

$$(a, 2m, \frac{a_1^2 - m}{a}, 2a_1, 2\sqrt{m}) \text{ is equal to the ideal unity,}$$

i.e., the integers are relatively prime. All the integers are

relatively prime in any ideal if three integers are relatively prime.

Assume that a and m are divisible by a prime number $q > 2$. Then $a_1^2 - m \equiv 0 \pmod{q}$ for $a_1^2 - m \equiv 0 \pmod{a}$ by hypothesis. Hence $a_1^2 \equiv 0 \pmod{q^2}$ since $m \equiv 0 \pmod{q}$.

But $\frac{a_1^2 - m}{a} \not\equiv 0 \pmod{q^2}$ since m has no quadratic factor. Therefore a, 2m and $\frac{a_1^2 - m}{a}$ do not have the same odd prime factor in common.

Suppose $q = 2$ and a and 2m are divisible by 2. By hypothesis m is odd, a is thus even. Therefore a_1 is odd. Hence $a_1^2 - m \equiv -2 \pmod{4}$ and $\frac{a_1^2 - m}{a}$, is odd. a, 2m and $\frac{a_1^2 - m}{a}$ are thus relatively prime. Hence the given ideal is equal to the ideal unity (1). Therefore $I_1 I_1' = a i_2^2 = (i i_2) = (N(I_1)$

Case 2. $m \equiv 2 \pmod{4}$.

In this case, as before $(a, a_1 + \omega)(a, a_1 + \omega') = (a)(a, 2m,$ $\frac{a_1^2 - m}{a}, 2a_1, 2\sqrt{m})$. As before a, 2m, $\frac{a_1^2 - m}{a}$ contain no odd prime. Furthermore they cannot contain the factor 2, for if,

$$a \equiv 0 \pmod{2} \text{ and } 2m \equiv 0 \pmod{2} \text{ then,}$$

$$a_1 \equiv 0 \pmod{2} \text{ and } a_1^2 \equiv 0 \pmod{4}.$$

Hence $a_1^2 - m \equiv -2 \pmod{4}$. We thus have again, a, 2m, and $\frac{a_1^2 - m}{a}$ relatively prime. We therefore have the same conclusions as in case 1.

Case 3. $m \equiv 1 \pmod{4}$ $\omega = \frac{1 + \sqrt{m}}{2}$, $\omega' = \frac{1 - \sqrt{m}}{2}$

$I_1 I_1' = (i_2^2)(a^2, 2aa_1 + a, a\sqrt{m}, (a_1 + 1)^2 - m)$
$(a_1 + \frac{1}{2})^2 - \frac{m}{4}$
$I_1 I_1' = (i_2^2)(a)(a_1, m, \frac{(a_1 + \frac{1}{2})^2 - \frac{m}{4}}{a}, 2a_1 + 1, \sqrt{m})$

As before we shall assume q an odd prime. Then,

$$a \equiv 0 \pmod{q} \text{ and } m \equiv 0 \pmod{q}. \text{ In a way}$$

similar to the above, we can prove that, $\frac{\frac{(2a_1 + 1)^2}{4} - \frac{m}{4}}{a} \not\equiv 0 \pmod{q}$

is odd. Hence the integers are again relatively prime· In all
three cases we have,

$$I_1 I_1' = (i_2^2)(a) = (ai_2^2) = (ii_2).$$
$$I_1 I_1' = (N(I_1)).$$

Definition.- A Prime Ideal is an ideal which is different from
the ideal unity and is divisible only by itself and the ideal
unity.

We now wish to show that an ideal can be resolved into
its prime factors, i.e., its prime ideals in only one way. In
order to do this it will be necessary to establish the follow-
ing theorems:-

Theorem IV.- If I_1, I_2 and I_3 are any three ideals different
from zero, such that $I_1 I_2 = I_1 I_3$ then $I_2 = I_3$.

If we multiply an ideal by its conjugate, we obtain a
principal ideal which is a rational number. Hence,

$$I_1 I_1' I_2 = I_1 I_1' I_3.$$

But since $I_1 I_1' = N(I_1)$, we have,

$$(\text{Ideal } N(I_1) I_2) = (\text{Ideal } N(I_1) I_3).$$

Taking out the common factor $(N(I_1))$, we get,

$$I_2 = I_3.$$

Theorem V. - If all the numbers of an ideal I_1 are congruent
to zero with regard to modulus I_2 then I_1 is divisible by I_2.

Let $I_1 = (\alpha_1, \alpha_2, \alpha_3, \text{------------})$

and $I_2 = (\beta_1, \beta_2, \beta_3, \text{---------------})$

then by hypothesis , $\alpha_1 \equiv 0 \pmod{I_2}$

$$\alpha_2 \equiv 0 \pmod{I_2}.$$

Multiplying I_1 and I_2 by the conjugate of I_2 we get $I_1 I_2'$

and $I_2 I_2' = (N(I_2))$

Now we wish to show that $I_1 I_2'$ is divisible by $I_2 I_2'$. From the

above congruence and the fact that,

$\beta_1' \equiv 0 (\text{mod. } I_2), \ \beta_2' \equiv 0 (\text{mod. } I_2),$ ----------------------

we get $\alpha_1 \beta_1' \equiv 0 (\text{mod. } I_2 I_2'), \quad \alpha_1 \beta_2' \equiv 0 (\text{mod. } I_2 I_2')$----------------

$\alpha_2 \beta_1' \equiv 0 (\text{mod. } I_2 I_2'), \quad \alpha_2 \beta_2' \equiv 0 (\text{mod. } I_2 I_2')$ ----- -------

----

Since $I_2 I_2' = (N(I_2))$ is a principal ideal and hence a ration-

al number, we can write,

$$\alpha_1 \beta_1' = N(I_2) \gamma_{11}, \alpha_1 \beta_2' = N(I_2) \gamma_{12}$$ -- ----------------------

$$\alpha_2 \beta_1' = N(I_2) \gamma_{21}, \alpha_2 \beta_2' = N(I_2) \gamma_{22}$$ ------- ----------------

----

----

where γ_{11}, γ_{12}, γ_{13}, γ_{14}, ----------------- , are integral numbers

of the field. From the above equations we may obtain,

$$I_1 I_2' = (N(I_2))(\gamma_{11}, \gamma_{12}, \gamma_{13}, -------------).$$

Now $(\gamma_{11}, \gamma_{12}, \gamma_{13}, ----------------)$ is equal to an ideal I_3

since it arose from taking the common factor $N(I_2)$ out of the

ideal $I_1 \bar{I}_2$. Hence we have from the above equation

$$I_1 I_2' = I_2 I_2' I_3 \quad \text{and by applying theorem IV}$$

we get, $\qquad I_1 = I_2 I_3$, i.e., I_1 is divisible by I_2.

Theorem VI.- If the product of two ideals $I_1 I_2$ is divisible

by I_3, and I_2 is prime to I_3 then I_1 is divisible by I_3.

Let $I_1 = (\alpha_1, \alpha_2, \alpha_3, ------------)$

and $I_2 = (\beta_1, \beta_2, \beta_3, -- --- ------)$ as before and

$I_3 = (\eta_1, \eta_2, \eta_3, -------------)$

Since by hypothesis I_2 is prime to I_3, then the greatest common divisor $I_2 + I_3 \equiv$ Ideal unity (1) .

Hence we can find two numbers β and π in I_2 and I_3 such that

$$\beta + \pi = 1.$$

Also by hypothesis $I_1 I_2$ is divisible by I_3, therefore the following congruences hold:-

$$\alpha_1 \beta_1 \equiv 0, \quad \alpha_2 \beta_1 \equiv 0 \quad ------------(\text{mod. } I_3)$$

$$\alpha_1 \beta_2 \equiv 0, \quad \alpha_2 \beta_2 \equiv 0 \quad ------------(\text{mod. } I_3)$$

$$------------------------------------$$

$$------------------------------------$$

$$\alpha_1 \beta \equiv 0 \quad \alpha_2 \beta \equiv 0 \quad ------------(\text{mod. } I_3)$$

Since $n \equiv 0$ (mod. I_3) , we may write,

$$\alpha_1 (\beta + \pi) \equiv 0, \quad \alpha_2 (\beta + \pi) \equiv 0 \quad ------------(\text{mod. } I)$$

Also since $(\beta + \pi) = 1$ the same relations hold.

Therefore it follows that,

$$\alpha_1 \equiv 0, \quad \alpha_2 \equiv 0 \quad -- ----------------- (\text{mod. } I_3), \text{ that is}$$

I_1 is divisible by I_3.

We are now in a position to prove the following theorem.

Theorem VII.- Every ideal can be separated into its prime factors in only one way.

Let any given ideal be,

$$I_4 \equiv I_{\alpha_1}, \; I_{\alpha_2}, \; I_{\alpha_3}, - ----------- . \; I_{\alpha_1}, \; I_{\alpha_2}, \; I_{\alpha_3}, -----$$

being prime ideals.

Suppose I_4 could be separated into its prime factors in another way, namely

$$I_4 \equiv I_{\beta_1}, \; I_{\beta_2}, \; I_{\beta_3}, ------------- . \; I_{\beta_1}, \; I_{\beta_2}, \; I_{\beta_3}, ------- \text{ being prime}$$

ideals. Let us consider first I_{α_1}. It must be contained in $I_{\beta_1}, \; I_{\beta_2}, \; I_{\beta_3}, ----------$. and hence is a divisor of I_{β_1}, or is

prime to I_{β_1} and therefore contained in the product I_{β_2}, I_{β_3}, I_{β_4}
---------- . In the latter case, either $I_{\alpha_1} = I_{\beta_2}$, or is con-
tained in the product I_{β_3}, I_{β_4}, --------- . Continuing this
reasoning , we see that I_{α_1} must equal some one of the I_{β}'s.
Similarly I_{α_2}, I_{α_3}, ---------. must each equal some I_{β}. Hence
the assumption that $I_4 \equiv I_{\beta_1}$, I_{β_2}, I_{β_3}, ----------- is different
from $I_4 = I_{\alpha_1}$, I_{α_2}, I_{α_3}, -------- , is false. It thus follows
that every ideal can be separated into its prime factors in
only one way.

Bibliography.

The following books were referred to, in the preparation of this thesis:-

Dirichlet- Vorlesungen Über Zahlentheorie·- Supplement XI.

Yahresbericht der Deutschen Mathematiker-Vereinigung. Vol. IV. Report by David Hilbert on " Die Theorie der Algebraischen Zahlkörper.

Allgemeine Arithmetik Der Zahlenkörper. Volume V. P. Bachmann.

Elements De La Theorie Des Nombres. - E. Cahen.

Encyklopadie Der Mathematischen Wissenschaften.

Repertorium Der Höheren Mathematik. Vol. I. Pascal.

Vorlesungen Über Zahlentheorie. Sommer.